Department of Homeland Security Daily Open Source Infrastructure Report for 10 August 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports BP North America's problem of corroding pipes is worsening as the nation's largest oil field ages and more water and less oil is produced during drilling. (See item 1)
- The Durango Herald reports the San Juan Basin Health Department says that the third human case of plague in the last five weeks has been reported in La Plata County, Colorado, causing concern. (See item 21)
- CNN reports immigration agents and the FBI are looking for 11 Egyptian students who entered the United States on valid student visas, then failed to show up at a university in Montana. (See item 31)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 09, Associated Press* — **Questions raised over aging oil fields.** BP North America's problem of corroding pipes is worsening as the nation's largest oil field ages and more water and less oil is produced during drilling. "Really, we are a giant water field," said Bill Hedges, BP PLC's corrosion expert, explaining that what comes up now during drilling is three−quarters

water. Water contains carbon dioxide, ideally suited to corroding pipelines. The Prudhoe Bay oilfield is very different now from what it was when it was first brought onstream, said ING analyst Jason Kenney. "The changing quality of the crude that is being produced has presented an issue with the infrastructure that's in place and the development and that is what BP are battling against," Kenney said. BP is spending $72 million this year on its anticorrosion program, with about half that money going for millions of gallons of corrosion inhibiting chemicals placed in the pipelines. The amount of inhibitor is roughly double what it was a decade ago. CSFB analyst Edward Westlake said the outage in Alaska confirms that some non−OPEC production infrastructure is becoming old.
Source: http://www.dfw.com/mld/dfw/business/15229850.htm

2. *August 08, Canadian Press* — **Canadian regulatory standards help mitigate energy pipeline corrosion, ruptures.** Regulatory standards in Canada have helped guard against the severe corrosion and leaks that have hobbled a major oil pipeline system in Alaska. BP announced Monday, August 7, it would temporarily shut down its Prudhoe Bay oil field in Alaska due to severe corrosion in a section of pipeline. Pipeline companies that operate in Canada are required to file an integrity management plan with the National Energy Board (NEB). Together they set safety standards for maintaining pipelines. The NEB then audits companies to ensure compliance. A report by the board released last March suggests the system is working well. The number of ruptures has declined since 1997, says the report. "There were no ruptures reported on NEB−regulated pipelines in 2003." While information on more recent years is still being tabulated, there have been no reports of any major ruptures or leaks, said Carole Leger−Kubeczek, an NEB board spokesperson.
Source: http://www.cbc.ca/cp/business/060808/b080898.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *August 09, ABC 7 (IL)* — **Hazmat crews respond to gas main break in Chicago.** People's Gas has secured a broken gas main on the Chicago's West Side. A construction crew reportedly struck the two−inch main at 2432 W. Lake Street. Trains were shut down from Clinton Street to Pulaski Road for a short time as a result.
Source: http://abclocal.go.com/wls/story?section=local&id=4444997

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *August 09, Scotsman (UK)* — **One in ten Britons suffers ID theft.** One in ten Britons has been the victim of identity fraud, according to new research which suggests the problem of stolen

personal information is much worse than previously thought. Nine percent of those interviewed for the study believed they had been a victim of ID theft −− the equivalent of six million people. Experts said the number of fraudulent incidents was far higher than reported. The most vulnerable were those under 30, because they are the least aware when it comes to protecting their personal information. According to CIFAS, the UK's fraud prevention service, identity theft has risen from 20,000 reported cases in 1999 to 137,000 in 2005. Professor Martin Gill, identity theft specialist and professor of criminology at Leicester University, said: "Official statistics relating to cases of ID theft are not indicative of the true scale of this growing crime, many cases go unrecorded or undetected.
Source: http://thescotsman.scotsman.com/index.cfm?id=1153962006

5. *August 08, Register (UK)* — **Phishing Trojan plays ping−pong with captured data.** Security researchers have identified a new Trojan which sends data back to attackers via an unconventional communications protocol (for malware) in a bid to escape detection. The as−yet unnamed phishing Trojan transmits stolen information back to hackers via ICMP (Internet Control Message Protocol) packets instead of e−mail or HTTP packets, the standard route for transmitting purloined information. After infecting a victim's computer, the Trojan is programmed to install itself as an Internet Explorer Browser Helper Object. The software then waits for a victim to post sensitive data online. This data, once entered, is captured by the Trojan and sent to attackers.
Source: http://www.theregister.co.uk/2006/08/08/phishing_trojan/

6. *August 08, Honolulu Advertiser (HI)* — **Hawaii credit union stops phishing scam.** Hawaii State Federal Credit Union was able to get a bogus Website shut down Monday, August 7, to prevent members from being scammed. The Website's link was included in a fraudulent e−mail spread over the Internet aimed at getting credit union members to divulge personal information. It was the first time Web thieves had targeted Hawaii State Federal members with an e−mail, the credit union said. Customers of other local institutions, including American Savings Bank, Bank of Hawaii, and First Hawaiian Bank have previously been targeted. The e−mail told recipients that their account information may have been obtained by outside parties and asked them to click on a link to go to a "secure site" where they could reactivate their account.
Source: http://the.honoluluadvertiser.com/article/2006/Aug/08/bz/FP6 08080322.html

7. *August 08, Finextra* — **Card skimmers steal from Copenhagen ATMs.** Three Romanian men have appeared in a Denmark court for creating fake debit cards and stealing cash from ATMs in Copenhagen. The group installed a small skimming device in a credit card reader at a bookshop in Copenhagen, which recorded information from customers' cards. This data was then copied to 'pre−pay' cards which were used at ATMs to steal funds from bank accounts. The gang used the fake debit cards 509 times over three days. In one instance, a suspect was able to withdraw money at the same ATM for nearly two hours.
Source: http://finextra.com/fullstory.asp?id=15695

8. *August 08, Register (UK)* — **Camera phones linked to South African bank theft muggings.** South African muggers are using camera phones to capture pictures of potential victims in banks before their accomplices stalk and rob them, according to reports. The ruse is helping street thieves in the Walmer district of Port Elizabeth to target well−heeled victims, according to police spokesperson Captain Verna Brink. "This way the person is not actually followed out

of the bank, and there is very little suspicion aroused," Brink said, the Herald reports. Local police are urging banks to prohibit the use of camera phones on their premises. Theft of a different sort −− fears over the use of camera phones to help low−level scammers make a clean getaway or to help thieves to case premises in preparation for armed robberies −− has prompted a number of U.S. banks to prohibit the use of mobiles on their premises. First National Bank branches in Chicago has joined with banks in Citizens Bank of Northern California and Indiana−based Citizens Financial Bank in banning the technology. Banks in Mexico City began banning mobiles in May as part of attempts to foil armed robberies, the Chicago Tribune reports.
Source: http://www.theregister.co.uk/2006/08/08/mobile_bank_mugging/

[Return to top]

Transportation and Border Security Sector

9. *August 09, Associated Press* — **Boston's Big Dig ramp reopens after nearby tunnel collapse.** A Big Dig ramp, closed amid safety concerns in the wake of the deadly collapse of a nearby tunnel ceiling, reopened shortly after midnight on Tuesday, August 8. A hotel van and about half a dozen cars were the first vehicles through the eastbound ramp that funnels traffic toward the Ted Williams Tunnel and Boston's Logan International Airport. It is key to easing traffic congestion originating south of the city. The ramp was closed shortly after an accident July 10 that killed Milena Del Valle, as she and her husband drove through a connector tunnel and their car was crushed by 12 tons of falling ceiling panels. Since the accident, authorities have zeroed in on the bolt−and−epoxy system that failed to hold suspended ceiling panels in place where she was killed. Inspections have revealed slippage in dozens of other tunnel locations, and workers have been reinforcing potentially weak connections. The U.S. Department of Transportation said the decision to reopen the ramp followed a thorough inspection of tunnel repairs. Other tunnel sections closed after the accident could take months to inspect and reopen, Governor Mitt Romney has said.
Source: http://www.usatoday.com/news/nation/2006−08−09−big−dig_x.htm

10. *August 09, Associated Press* — **Airlines continue to look overseas.** The nation's biggest airlines continued to shift their focus overseas in July, pulling seats from the domestic market and putting them on more profitable international routes, according to carriers' most recent traffic reports. Overall domestic capacity of the six biggest traditional hub−and−spoke carriers fell 6.4 percent in July, while their international capacity grew at a six percent clip. The continued trend means international routes now make up over a third of the big six's total capacity, up to 36 percent from 33 percent a year ago. Internationally, four of the big six airlines reported capacity gains. Overall, the strongest gains for the big six were in European and Latin American routes. Capacity to Asia declined 1.5 percent compared with last July. Carriers, though, have recently been showing more of an appetite for service to China. American Airlines in July said it's seeking permission for a second route to China, hoping to offer daily nonstop service between Dallas and Beijing beginning in March.
Source: http://biz.yahoo.com/ap/060808/airlines_traffic_roundup.html ?.v=1

11. *August 09, Naples Daily News (FL)* — **Man arrested at airport led police on chase.** A man arrested Tuesday night, August 8, for driving on a runway at Southwest Florida International

Airport had just outrun police during a short car chase. A Lee County Sheriff's deputy responded to a disturbance call at the home that Jack Brems, 34, shares with his mother Dorothy about an hour before the Fort Myers, FL, man broke through an airport gate and drove onto a runway. Lee County Port Authority police arrested Brems at 7:15 p.m. EDT after he lead officers on a 15−minute chase around the airport's runway.
Source: http://www.naplesnews.com/news/2006/aug/09/man_arrested_airport_led_police_chase/?latest

12. *August 09, Daily Nonpareil (IA)* — **Three southwest Iowa airports receive funding.** Red Oak, Shenandoah, and Harlan Municipal airports were granted a total of $374,060 by the Iowa Transportation Commission (ITC) to complete vertical infrastructure projects in 2007. In all, the ITC approved $3 million to the Iowa State Aviation Program. The program will provide nearly $2.4 million of those funds for vertical infrastructure projects at eight commercial service airports and 12 general aviation airports in Iowa. An additional $688,000 will provide funding for Airport Improvement Program projects, including: airfield and security projects at 10 general aviation airports, aviation safety programs, and planning studies. Red Oak Municipal Airport, with $216,000, received the largest grant of the 30 airports that were granted funds. That money will go toward construction of a 100− by 100−foot hangar for corporate aircraft.
Source: http://www.zwire.com/site/news.cfm?newsid=17032184&BRD=2703&PAG=461&dept_id=555106&rfi=6

13. *August 09, Reuters* — **Scare over package disrupts Washington, DC rail service.** An empty package on the tracks of Washington's Metro rail system caused a security scare that tied up morning commuter traffic for three hours in the heart of the U.S. capital on Wednesday, August 9, authorities said. The package, a square−foot plastic box, was found near Amtrak's Union Station about 9:10 a.m. EDT along a track bed that the Washington Metropolitan Area Transit Authority shares with the national passenger rail service. A police bomb squad, with FBI agents standing by, blasted the package open with a water cannon shortly before midday. "They found out it was just an empty box. We don't know how it got there but it's all over," said Metro spokesperson Taryn McNeil.
Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyID=2006−08−09T171342Z_01_N09387790_RTRUKOC_0_US−SECURITY−WASHINGTON.xml&WTmodLoc=NewsHome−C3−domesticNews−3

14. *July 10, Government Accountability Office* — **GAO−06−820R: Active Commuter Rail Agency Service Contracts (Correspondence).** In correspondence to the Committee on Banking, Housing and Urban Affairs of the United States Senate, the Government Accountability Office said it was asked to provide information on the service arrangements between commuter rail agencies and other companies. Accordingly, we addressed the following questions: (1) How many currently active commuter rail service contracts were obtained through competitive and noncompetitive processes? (2) What differences, if any, are there between competitively and noncompetitively negotiated contracts? Through interviews and site visits with commuter rail agencies, we identified all 50 active commuter rail contracts that provided at least one of the four following services: train operations, MOE, dispatching, and MOW. Of these 50 contracts, we found that 22 only provided access to infrastructure and services directly related to maintaining and operating the infrastructure. These contracts did not include other services, such as train operations, that are not bound to the infrastructure and for

which a commuter rail agency could choose a provider other than the infrastructure owner. Our review did not examine commuter rail agencies' compliance with the Federal Transit Administration's requirements for the use of competitive procurement for railroad service contracts. We conducted our review from July 2005 to July 2006 in accordance with generally accepted government auditing standards
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−820R

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *August 09, Agence France−Presse* — **China reports new foot−and−mouth outbreak.** China has reported a fresh outbreak of foot−and−mouth disease, with 230 head of cattle affected in the northwestern province of Gansu. Cattle in Gansu's Huining County began showing symptoms on July 31 and were diagnosed with foot−and−mouth disease Friday, August 4. A total of 607 sheep, pigs and cattle, including the sick animals, were culled following the outbreak, while local agriculture officials quarantined and disinfected the farms and surrounding area. Foot−and−mouth is a severe and highly contagious viral disease affecting cattle, pigs, sheep and other livestock.
Source: http://news.yahoo.com/s/afp/20060809/hl_afp/healthchinafarm_060809142548

16. *August 09, Agricultural Research Service* — **Russian bees more resistant to mites.** The bee has had a rough time of it lately. Parasitic mites are beating down this insect that's crucial for producing more than $15 billion worth of U.S. crops each year. But according to scientists with the Agricultural Research Service (ARS), there's hope for American bees. It comes from the hills of southeast Russia. According to recent studies done at the ARS Honey Bee Breeding, Genetics and Physiology Research Unit, Russian bees are capable of deflecting three of the honeybee's worst assailants: varroa mites, tracheal mites and cold temperatures. Ten years ago, ARS bee researchers led by Thomas Rinderer trekked through Russia's Primorsky Territory in search of bees that could naturally hold their own against varroa mites. There, bees have become battle−hardened against the blood−sucking mite, which has been harassing Russian bees for more than 150 years. Since Russian bees were first imported by Rinderer, they have continued to impress researchers. In fact, ARS entomologist Jose Villa recently discovered just how the bees fend off tracheal mites, which kill honey bees by invading and clogging their airways. Villa and fellow ARS entomologist Lilia De Guzman have also confirmed that Russian bees are excellent cold−weather survivors.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Food Sector

17. *August 09, Reuters* — **More Indian states ban colas.** Two southern Indian states banned the sale of soft drinks produced by Coca−Cola and Pepsi on Wednesday, August 9, after an environmental group said it had found pesticides in the companies' products. While the coastal state of Kerala announced a blanket ban on the production and distribution of the two soft drinks, its neighbor Karnataka banned them from schools, colleges and hospitals, officials said. Three states previously imposed bans similar to the one in Karnataka after the Delhi−based Center for Science and Environment said it had found an average pesticide residue of 11.85 parts per billion in 57 samples of Coca−Cola and PepsiCo drinks produced in 12 Indian states. Those pesticide levels are 24 times higher than limits agreed, but not yet enforced, by the Bureau of Indian Standards.
Source: http://today.reuters.com/news/articlenews.aspx?type=scienceNews&storyID=2006−08−09T113213Z_01_DEL337859_RTRUKOC_0_US−INDIA−COLAS.xml&archived=False

[Return to top]

Water Sector

18. *August 08, San Diego Union−Tribune* — **Boil−water advisory methods.** San Diego, CA, officials did everything by the book last weekend when they issued the city's first−ever order for boiling water to kill bacteria, then lifted it a day later, state health officials said Monday, August 7. But the public notification system for about 120,000 people affected by the contamination proved so hit−and−miss that Mayor Jerry Sanders has asked his top deputies to find better ways to tell people about similar emergencies. Sanders held a news conference to alert people about the contamination and boil−water order. Some residents didn't learn about the order until shortly before it was lifted. City officials said they considered various notification options but were constrained by California regulations. For example, the water problem didn't meet state standards for using electronic freeway signs or the emergency alert system broadcast over radio and television. San Diego water department Director Jim Barrett acknowledged that his agency needs to find new communication methods in case people don't check the city's Website or watch the evening news.
Source: http://www.signonsandiego.com/news/northcounty/20060808−9999 −1n8boil.html

[Return to top]

Public Health Sector

19. *August 09, Agence France−Presse* — **Thailand declares bird flu a national threat.** Thailand has declared bird flu a national threat and vowed united efforts to tackle the deadly virus. Thailand has suffered 24 human cases of bird flu, including 16 fatalities, since the disease was first detected in the country in early 2004. On Tuesday, August 8, it declared more than one third of the country, including Bangkok, a disaster zone as a precaution to help local officials battle the virus.
Source: http://news.yahoo.com/s/afp/20060809/hl_afp/healthfluthailand_060809101859;_ylt=Ajmx0lN4Xks6HKCMehVVYiCJOrgF;_ylu=X3oDMT

A5aHJvMDdwBHNlYwN5bmNhdA−−

20. *August 08, Associated Press* — **Turkey fights Ebola−like fever outbreak.** Turkey is battling the largest recorded outbreak of Crimean−Congo Hemorrhagic Fever, which has killed at least 20 people this year, and experts said Tuesday, August 8, more cases of the Ebola−like disease are inevitable in coming months. Most of the cases have occurred in six provinces in the Black Sea and Central Anatolia region: Tokat, Sivas, Gumushane, Amasya, Yozagat and Corum. Authorities at the World Health Organization are awaiting further information from the Turkish government, including where the other cases have arisen. Turkish authorities say no cases have been reported in the tourist areas along the Mediterranean coast. By August 4, there were 242 cases of the disease, including 20 deaths, making it the largest reported outbreak since it was first identified in 1944, authorities said.
Crimean−Congo fever information:
http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/cchf.htm
Source: http://abcnews.go.com/International/wireStory?id=2288571

21. *August 08, Durango Herald (CO)* — **Plague again hits county, draws concern.** The third human case of plague in the last five weeks has been reported in La Plata County, CO, according to the San Juan Basin Health Department. The male patient was released from the hospital after several days and is recovering at home, said Lynn Westberg, the executive director of the Health Department. While it is the third case of the plague in the county in 2006, there have been five human cases in the last 12 months. "I am quite concerned by the situation in La Plata County right now," said Joe Fowler, regional epidemiologist for the Health Department. "The entire state of Colorado has never had more than four cases in a single year, but this year, if our residents do not take precautions to protect themselves, La Plata County could single−handedly surpass that number."
Plague information: http://www.cdc.gov/ncidod/diseases/submenus/sub_plague.htm
Source: http://durangoherald.com/asp−bin/printable_article_generation.asp?article_path=/news/06/news060808_4.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *August 09, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: A low pressure center about 700 miles east of the Windward Islands is moving west at 12−18 mph. This low center is weakening and its threat to develop into a tropical cyclone during the next 36 hours is becoming less likely with time. Western Pacific: There are three tropical systems in the Western Pacific; Typhoon 08W (Saomai), Tropical Storm 09W (Maria) and Tropical Storm 10W (Bopha). They pose no threat to U.S. territories. Earthquake Activity:

The most significant earthquake during the last 24 hours was a magnitude 3.3 (Minor) earthquake near Mount St. Helens in Washington at 11:01 EDT Tuesday, August 8.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat080906.shtm

23. *August 09, Providence Journal (RI)* — **Rhode Island readies for the next hurricane.** For the first time, the Federal Emergency Management Agency (FEMA) is storing supplies on Block Island, RI, in anticipation of the hurricane season. And it's the first time that FEMA has prepositioned supplies anywhere in New England, said FEMA Region 1 Director Arthur Cleaves. Rhode Island and Massachusetts are the only New England states where FEMA is stocking food, water, and shelter supplies. "Rhode Island is the only one to date to take advantage of the partnership with FEMA," said Cleaves. The shelter container, which is being stored at the Block Island School, holds a generator, wheelchairs, plus enough blankets and cots for 250 people. The trailer, which has 7,000 meals−ready−to−eat and 3,300 bottles of water, is being stored at the airport. Meanwhile, the governor's office is mailing out 300,000 pamphlets this week containing evacuation maps, shelter information, and safety tips and emergency contacts to residents living in coastal communities. The maps show the areas that would be flooded by a hurricane, as well as the evacuation routes and current shelters approved by the Red Cross.
Source: http://www.projo.com/ri/southkingstown/content/projo_20060809_bievac.219db37.html

24. *August 08, Illinois Government News Network* — **Illinois' State Weapons of Mass Destruction Team demonstrates capability to take down terrorist groups.** The State of Illinois' large−scale terrorist response exercise concluded Tuesday morning, August 8, in the Metro East as the State Weapons of Mass Destruction Team (SWMDT) successfully demonstrated its ability to take down a mock terrorist group responsible for several simulated attacks staged during the exercise. The scenario was part of a multi−day exercise that brought together responders from federal, state and local agencies to test response to multiple disaster scenarios. Illinois' emergency response exercise began Friday morning with a mock rail yard explosion scenario in Edwardsville that triggered an evacuation and sheltering exercise of area residents. As part of the scenario, local law enforcement discovered evidence of explosives. In response, Governor Rod Blagojevich, as part of the exercise, ordered several actions to protect citizens, including calling up Illinois National Guard troops, increasing security at critical infrastructure in the Metro East area and declaring a state disaster declaration. The governor also approved deploying the SWMDT, which followed up on intelligence reports gathered throughout the exercise to locate and take down the terrorist group. "The state weapons of mass destruction team's quick, effective response in this exercise scenario shows that we have the capacity to take down terrorists," said Governor Blagojevich.
Source: http://www.illinois.gov/PressReleases/ShowPressRelease.cfm?SubjectID=1&RecNum=5161

[Return to top]

Information Technology and Telecommunications Sector

25.

August 08, U.S. Computer Emergency Readiness Team — **US−CERT Technical Cyber Security Alert TA06−220A: Microsoft products contain multiple vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Office, Works Suite, Visual Basic for Applications, and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. The update for MS06−040 addresses a critical vulnerability in the Windows Server service. US−CERT has received reports of active exploitation of this vulnerability.
Systems Affected: Microsoft Windows; Microsoft Office (Windows and Mac); Microsoft Works Suite; Microsoft Visual Basic Basic for Applications (VBA); Microsoft Internet Explorer.
Solution: Microsoft has provided updates for these vulnerabilities in the August 2006 Security Bulletins: http://www.microsoft.com/technet/security/bulletin/ms06−aug. mspx
When prioritizing updates, it is strongly encouraged to apply the update for MS06−040 first. Updates for Microsoft Windows and Microsoft Office XP and later are available on the Microsoft Update site. Microsoft Office 2000 updates are available on the Microsoft Office Update site: https://update.microsoft.com/microsoftupdate/v6/muoptdefault .aspx?ln=en&returnurl=https://update.microsoft.com/microsoft update/v6/default.aspx?ln=en−us
Apple Mac OS X users should obtain updates from the Mactopia Website: http://www.microsoft.com/mac/
System administrators may wish to consider using Windows Server Update Services: http://www.microsoft.com/windowsserversystem/updateservices/ default.mspx
Source: http://www.uscert.gov/cas/techalerts/TA06−220A.html

26. *August 08, Time* — **How Hezbollah hijacks the Internet.** Hackers from the militant Lebanese group Hezbollah are trolling the Internet for vulnerable sites to communicate with one another and to broadcast messages from Al−Manar television. In today's asymmetrical warfare, the Internet is vital to groups like Hezbollah who use it to recruit, raise money, communicate and propagandize. The recent hijacking of a South Texas cable operator is a case study in how Hezbollah moves in. The Texas cable company has an agreement with a New York−based satellite communications aggregator, which moves feeds to a variety of customers from throughout the world, including Lebanon. A technician in New York made an improper connection and that opening was detected by Hezbollah. Al−Manar linked to the small cable company's Internet Protocol (IP) address, which can be thought of, in simple terms, as a telephone number. Hezbollah essentially added an extension on that telephone line allowing their traffic to flow. Hezbollah then gets the word out through e−mail and blogs that it can be found at that IP address and the hijack is complete.
Source: http://www.time.com/time/world/article/0,8599,1224273,00.htm l

27. *August 08, Associated Press* — **Sprint Nextel to form network with WiMax.** Sprint Nextel Corp., the nation's third−largest cellular provider, said Tuesday, August 8, it will use an emerging technology called WiMax to build a new high−speed wireless network. The company said the new network, expected to launch in some markets by late 2007, will provide customers with wireless Internet speeds on par with DSL and cable TV modems and four times faster than speeds available on current wireless networks. The new WiMax network would provide download speeds of between 2 megabits per second and 4 mbps. That's in the same range as

today's typical broadband offerings over phone and cable wires, but considerably slower than the speeds those providers are starting to offer as they upgrade their networks. WiMax has been touted as a "next big thing" in wireless technology for several years, but actual deployments around the world have mostly been limited to small trials rather than full−blown network launches. Though derived from the same technology as the popular Wi−Fi standard that provides wireless Internet access in such places as airports and coffee shops, a WiMax signal can blanket a much wider coverage area.
Source: http://news.yahoo.com/s/ap/20060809/ap_on_hi_te/sprint_nextel_wimax;_ylt=AqIBcqbbMSO69L3QkrxbmSkjtBAF;_ylu=X3oDMTA2Z2szazkxBHNlYwN0bQ−−

28. *August 08, Associated Press* — **FCC auctions off rights to airwaves.** The government has auctioned off rights to the largest chunk ever of mobile−phone−friendly airwaves. The auction, conducted Wednesday, August 9, by the Federal Communications Commission (FCC), may lead to an expansion of advanced services for mobile wireless customers, like super−fast Internet access. In addition, the new spectrum could allow satellite companies to offer wireless broadband access to customers along with their usual video services.
Source: http://news.yahoo.com/s/ap/20060809/ap_on_hi_te/selling_the_airwaves;_ylt=Avo6cQ1jjz3iDXzWrafqzDMjtBAF;_ylu=X3oDMTA2Z2szazkxBHNlYwN0bQ−−

29. *August 04, IDG News Service* — **Serious flaw puts Xerox printers at risk.** Xerox Corp. is scrambling to update a security patch following the disclosure of a major security flaw in its WorkCenter multifunction printers. By taking advantage of a configuration error in the printers' Web interface, security researcher Brendan O'Connor was able to run unauthorized software on the printers, compromise network traffic and access sensitive information being printed on the machines. He shared details of how to compromise the printers during a presentation at the Black Hat USA conference in Las Vegas Thursday, August 3. O'Connor said he was not trying to "pick on Xerox," but rather using his hack as a case study to draw attention to the security threat posed by increasingly powerful embedded devices.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002199&source=rss_topic85

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 445 (microsoft−ds), 32790 (−−−), 80 (www), 113 (auth), 20282 (−−−), 135 (epmap), 6346 (gnutella−svc), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *August 08, Associated Press* — **FBI says "suspicious" packages at synagogues were harmless.** Suspicious packages received at four Pittsburgh synagogues contained no bombs or other harmful substances, the FBI said Tuesday, August 8. The packages were reported as suspicious because they had no return addresses. But FBI Special Agent Jeff Killeen said they contained literature and CDs that appeared to be part of an informational mass mailing. Some of the information was in Hebrew, which authorities had not immediately translated, Killeen said. "Because of the volatile situation in the Middle East, everybody responded promptly," Killeen said. "Those who received the material thought the items were suspicious, so they reported it as they should."
Source: http://www.phillyburbs.com/pb−dyn/news/103−08082006−695126.h tml

[Return to top]

General Sector

31. *August 09, CNN* — **Egyptian students disappear in U.S.** Immigration agents and the FBI are looking for 11 Egyptian students who entered the United States on valid student visas, then failed to show up at a university in Montana, authorities said. The FBI on Saturday, August 5, issued a nationwide alert to law enforcement agencies. Included were the students' names, ages, passport numbers and photographs. "At the present time there are no known associations to any terrorist groups. Approach with caution," the lookout bulletin states U.S. authorities are working with foreign intelligence agencies to make sure there is nothing suspicious in the students' backgrounds, federal sources said. Those sources added that 20 students applied for student visas to go to Montana State, but three of the applicants were denied.
Source: http://www.cnn.com/2006/US/08/08/egyptian.students/index.htm l

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer